WHAT IS CLAIMED IS:

1. A system for enforcing data stream continuity comprising:

a server coupled to a transmission link for providing a data stream to at least one client over the transmission link, the data stream being segmented into units, the server including:

a scrambler for encrypting at least one first unit using an encryption key;

a steganographic unit for embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

2. The system as recited in claim 1, wherein the steganographic unit employs a steganographic masking algorithm.

3. The system as recited in claim 1, wherein the data stream includes a transmission order which alternates between first units and second units.

4. The system as recited in claim 1, wherein the steganographic unit encrypts the at least one second unit.

5. The system as recited in claim 1, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

6. The system as recited in claim 1, wherein the transmission link includes the Internet.

7. The system as recited in claim 1, wherein at least one of the client and the server include a memory storage device.

8. A system for enforcing data stream continuity comprising:

a client system coupled to a transmission link for receiving a data stream from at least one server over the transmission link, the data stream being segmented into units, the client system including:

a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key;

a descrambler for descrambling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server; and

a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream.

9. The system as recited in claim 8, wherein the data stream includes a transmission order which alternates between first units and second units.

10. The system as recited in claim 8, wherein the encryption key is also steganographically hidden in the at least one second unit.

11. The system as recited in claim 8, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

12. The system as recited in claim 8, wherein the transmission link includes the Internet.

13. The system as recited in claim 8, wherein at least one of the client and the server include a memory storage device.

14. A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key;

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

15. The method as recited in claim 14, wherein the data stream includes a transmission order which alternates between first units and second units.

16. The method as recited in claim 14, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

17. The method as recited in claim 14, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

18. The method as recited in claim 14, wherein the link includes the Internet.

19. The method as recited in claim 14, wherein at least one of the client and the server include a memory storage device.

20. A method for enforcing data stream continuity comprising the steps of:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream.

21. The method as recited in claim 20, wherein the data stream includes a transmission order which alternates between first units and second units.

22. The method as recited in claim 20, wherein the step of steganographically embedding includes the step of steganographically embedding portions of the encryption key in the at least one first unit.

23. The method as recited in claim 20, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

24. The method as recited in claim 20, wherein the link includes the Internet.

25. The method as recited in claim 20, wherein at least one of the client and the server include a memory storage device.

26. A method for enforcing data stream continuity comprising the steps of:

providing data segmented into units for a data stream transferred over the link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling the at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

27. The method as recited in claim 26, wherein the data stream includes a transmission order which alternates between first units and second units.

28. The method as recited in claim 26, wherein the portions of the encryption key are embedded in the at least one first unit.

29. The method as recited in claim 26, wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key.

30. The method as recited in claim 26 wherein the link includes the Internet.

31. The method as recited in claim 14, wherein at least one of the client and the server include a memory storage device.

32. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

segmenting data to be transmitted over a link into units for a data stream to be transferred over the link;

scrambling at least one first unit for the data stream before transmission by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream;

extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling at least one first unit which was encrypted in accordance with the encryption key; and

reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.

33. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

providing data to be transmitted over a link;

segmenting the data into units for a data stream to be transferred over the link;

scrambling at least one first unit by encrypting the at least one first unit using an encryption key; and

steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream.

34. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enforcing data stream continuity, the method steps comprising:

providing data segmented into units for a data stream transferred over the link, the units including at least one first unit and at least one second unit;

extracting an encryption key steganographically embedded in the at least one second unit in the data stream;

descrambling the at least one first unit which was encrypted in accordance with the encryption key; and reassembling the data stream at the client such that all of the units of the data stream are needed to decipher the data stream.